NUI Galway
OÉ Gaillimh

Autumn Examinations 2016/2017

Exam Code(s)	4BCT1, 1MECE1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	Yes
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Dr. M. Schukat *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	X	No	
MCQ	Yes		No	X
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes		No	X

PTO

1 (a) Explain how a nonce can be used to provide evidence of freshness in a communication between two parties (9 marks)

(b) Outline how any dynamic password scheme (e.g. challenge response) that you are familiar with can be used to provide evidence of identity in a communication between two parties (8 marks)

(c) In the absence of mutual trust, a zero knowledge scheme for entity authentication might be deployed. Outline how such a scheme works, using any analogy of your own choice. (8 marks)

2 (a) List any four criteria that a forensic investigative technique should satisfy in order to have confidence that evidence supplied by the investigative technique is reliable. (8 marks)

(b) Discuss the process of disk imaging, explaining the term 'write blocker' in the course of your answer(9 marks)

(c) Outline any two challenges that you think face digital forensics through the emergence of mobile devices (8 marks)

3
Consider the document ‘Framework for Improving Critical Infrastructure Cybersecurity’, released by the National Institute of Standards and Technology (NIST) as draft version 1.1 in January 2017. The framework presented in this document is, as stated in the document, a ‘risk-based approach to managing cybersecurity risk’. Give your understanding of this framework under the three headings ‘Framework Core’ (9 marks), ‘Framework Implementation Tiers’ (8 marks) and ‘Framework Profile’ (8 marks).

4 (a) Give any two security properties that a hash function should satisfy, and briefly indicate any application area where in your view any one such security property is needed (9 marks)

(b) What does a message authentication code (MAC) offer that a hash function does not in your view? (8 marks)

(c) Sketch how a MAC scheme could be used to provide for digital signatures, assuming the existence of a trusted third party (arbitrator) (8 marks)

5 (a) By considering the plaintext ‘011100’ and an associated key ‘000000’, explain the principle underlying encryption and decryption for a simple stream cipher that depends on a randomly generated keystream and XOR (8 marks)

(b) ‘Block ciphers work on blocks rather than bits’. With the aid of a diagram, show one encryption round for the AES block cipher (8 marks)

(c) Consider a security solution that provides a confidentiality service via a block cipher deployed in Cipher Block Chain (CBC) mode and also an integrity service delivered via so-called ‘CBC-MAC’. Discuss whether this scheme is vulnerable to a Message Authentication Code (MAC) forgery attack if the same key is used for both the confidentiality service and the integrity service. You may assume that a message consists of N blocks and that an attacker has changed all enciphered blocks apart from the last one (9 marks)

6 (a) In the context of a public key encryption scheme such as RSA, explain what is meant by the terms ‘Certification Authority’, ‘Registration Authority’ and ‘Digital Certificate’ (9 marks)

(b) Sketch in outline how an RSA digital signature scheme with appendix works (8 marks)

(c) Explain in your own words what is meant by the idea that public key encryption and public key digital signature have complementary requirenments. Make use of the terms 'sign', 'verify' 'encrypt' and 'decrypt' in the course of your answer (8 marks)